UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/749,820	12/31/2003	Michael D. Kotzin	CS22914RA	9362

20280 7590 04/05/2007		

MOTOROLA INC
600 NORTH US HIGHWAY 45
ROOM AS437
LIBERTYVILLE, IL 60048-5343

EXAMINER
LE, CANH

ART UNIT	PAPER NUMBER
2139	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/05/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

PTOL-90A (Rev. 10/06)

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>30 January 2007</u>.

2a)☒ This action is **FINAL**.　　2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-2, 4-11, 13-17</u> is/are pending in the application.

　　4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-2,4-11 and 13-17</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

　　Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

　　Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

　　a)☐ All　b)☐ Some * c)☐ None of:

　　　1.☐ Certified copies of the priority documents have been received.

　　　2.☐ Certified copies of the priority documents have been received in Application No. _____.

　　　3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

　　* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
　　Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
　　Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

Claims 3 and 12 have been cancelled.

Claims 1-2, 4-11, and 13-17 have been examined and are pending.

Response to Amendment

The applicant's amendment filed January 30, 2007 necessitated the new

ground(s) of rejection presented in this Office action. Therefore, applicant's arguments

with respect to claim 1-2, 4-11, and 13-17 have been considered but are moot in view of

the new ground(s) of rejection.

Accordingly, THIS ACTION IS MADE FINAL. See MPEP 706.07(a). Applicant is

reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

Specification

The use of the trademarks of Sun, Hewlett Packard, Dell, Windows, LINUX,

UNIX have been noted in this application. It should be capitalized wherever it appears

and be accompanied by the generic terminology.

Although the use of trademarks is permissible in patent applications, the

proprietary nature of the marks should be respected and every effort made to prevent

their use in any manner which might adversely affect their validity as trademarks.

Please accompany all trademark names with their respective ™ symbol.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-2, 4-11, and 13 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Malinen et al. (Publication Number: US 2003/0028763 A1) and

Brown et al. (US Patent 5,668,875) in view of Blom (US 2003/0233546 A1).

Claim 1

Malinen teaches a method of authenticating an electronic device, the electronic device

having device specific identifying data stored therein, the method comprising:

obtaining one of the challenge response pairs associated with the electronic

device *[par. [0083], lines 7-12; par. [0011], lines 1-3; "an authentication gateway 115*

maintains an authentication session and is able to query the RAND (i.e. challenge) and

SRES (i.e. system response) for a received International Mobile Subscriber Identifier

(IMSI) from a local authorization database. An identity associated with a client is

equivalent to the device specific"];

communicating a challenge portion of the challenge response pair to the

electronic device *[par. [0011], lines 1-5; the challenge is sent to the client].*

receiving from the electronic device a response to the challenge portion, wherein

the response being based upon the device specific identifying information *[par. [0011],*

lines 5-6; a client generates a response that is sent back to the authorizer].

comparing the response to a response portion of the challenge response pair
[par. [0011], lines 6-7; an authorizer compares the challenge to the response]; and

authenticating the user if the response matches *[par. [0011], lines 8-9; If the
response is correct, the authorizer provides a service to the client]*.
Malinen does not teach a method of plurality of random challenges to the electronic
device and receiving a plurality of responses from the electronic device.

Brown teaches a method of issuing a plurality of random challenges to the
electronic device and receiving a plurality of responses from the electronic device,
wherein each random challenge and corresponding response represents a challenge
response pair which is unique and based upon specific identifying data of the electronic
device *[col. 4, line 66 to col.5 line 3; col. 11, lines 14-17; a RAND generator 136 is used
for generating the challenges in communication with the subscribe unit 110. Once the
responses are received at VLR, the MSI, location, service request and RAND/RESP$_v$
pairs are forward to home system and home location register or other authenticating
center for the user identity unit"]*;

Thus, it would have been obvious to the person of ordinary skill in the art at the
time the invention was made to modify the method of Malinen by including the step of
Brown because it would allow a subscriber and its associated home system
authentication protocol, and a roamed system uses a corresponding local authentication
protocol *[Blom, par. [001], lines 3-7]*.

Claim 2

Malinen also teaches the method of claim 1, wherein the step of obtaining <u>one of the</u>

challenge response pairs comprises obtaining from a database store of challenge

response pairs the challenge response pair *[par. [0083], lines 7-12; an authentication*

gateway 115 maintains an authentication session and is able to query the RAND (i.e.

challenge) and SRES (i.e. response) for a received International Mobile Subscriber

Identifier (IMSI) from a local authorization database. The local database can be used to

store more than one challenge response pair].

Claim 4

Blom further teaches the method of claim 1, wherein the step of obtaining a challenge

response pair comprises obtaining a challenge response pair from a challenge

response pair broker *[par. [0059], lines 11-14; a broker acting as a general*

authentication center or service provider].

Claim 5

Malinen further teaches the method of claim 1, wherein the device specific identifying

data comprises data stored on a subscriber identity module (SIM) card associated with

the electronic device, or computed by the SIM card upon demand

[par. [0074], lines 11-13. A SIM card provides a session key for the mobile node, and a

response is sent back to an authorizer].

Claim 6

Malinen further teaches the method of claim 1, comprising the step of discarding the

challenge response pair after use *[par. [0194]; a router advertisement contains a*

"challenge", which is essentially a random number used as a nonce].

Claim 7

Malinen further teaches the method of claim 1, wherein the step of obtaining a

challenge response pair comprises obtaining via a secure communication interface the

challenge response pair *[par. [0073]; par. [0074]; a client can use its own generated*

instance of the session key for secure communication with access provider. It is

included to obtain a challenge response pair].

Claim 8

Claim 8 is essentially the same as claim 1 except that it sets forth the claimed invention

as a system further comprising a memory for storing the challenge response pair *[see*

Malinen, par. [0083], lines 7-12; a memory is equivalent to a database] rather a method

and rejected under the same reasons as applied above.

Claim 9

Malinen further teaches the system of claim 8, wherein the device specific identifying

data comprises subscribed identity module (SIM) card data from a SIM card within the

electronic device *[par. [0074], lines 10-13]*.

Claim 10

Malinen further teaches the system of claim 9, wherein the user comprises a service

provider having a need to authenticate the electronic device *[par. [0074], lines 10-13]*.

Claim 11

Malinen further the system of claim 10, wherein the agent for interrogating and the

agent for providing are associated with the service provider *[par. [007], lines 2-4]*.

Claim 13

Blom further teaches the system of claim 8, wherein the agent for providing the

challenge response pair comprises a challenge response pair broker *[par. [0059], lines

11-14; a broker acting as a general authentication center or service provider]*.

**Claims 14-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Malinen et al. (Publication Number: US 2003/0028763 A1) and Brown et al. (US

Patent 5,668,875) in view of Ekberg (International Publication Number: WO

00/02406) and further in view of Blom (US 2003/0233546 A1).**

Claim 14

Malinen teaches a method of providing an authentication service comprising the steps

of:

        providing responsive to a request for an authentication service a challenge

response pair to a service provider for authenticating the electronic device by

communicating a challenge portion of the challenge response pair to the electronic

device *[par. [0011], lines 1-5; the challenge is sent to the client]*, receiving from the

electronic device a response to the challenge portion *[par. [0011], lines 5-6; a client

generates a response that is sent back to the authorizer]*, wherein the response being

based upon the device specific identifying information, comparing the response from the electronic device to a response portion of the challenge response pair *[par. [0011], lines 6-7; an authorizer compares the challenge to the response]*; and authenticating the user if the response matches *[par. [0011], lines 8-9; If the response is correct, the authorizer provides a service to the client]*.

Malinen does not teach a method of obtaining from an electronic device a plurality of challenge response pairs through issuance of a plurality of random challenges to the electronic device and receiving a plurality of responses from the electronic device.

Brown teaches a method of obtaining from an electronic device a plurality of challenge response pairs through issuance of a plurality of random challenges to the electronic device and receiving a plurality of responses from the electronic device, wherein each random challenge and corresponding response represents a challenge response pair which is unique and based upon the challenge and device specific identifying data associated with the electronic device *[col. 4, line 66 to col.5 line 3; col. 11, lines 14-17; a RAND generator 136 is used for generating the challenges in communication with the subscribe unit 110. Once the responses are received at VLR, the MSI, location, service request and RAND/RESP_v pairs are forward to home system and home location register or other authenticating center for the user identity unit"]*; Malinen and Brown do not teach for storing the challenge response pairs.

Ekberg teaches a method of storing the challenge response pairs *[abstract, lines 15-13; pg. 14, lines 27-37; pg. 15 lines 1-9; a subscriber-specific information is stored in*

a database (DB) in advance. A subscriber's authentication is contained at least a

challenge and a response];

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to combine the method of Malinen, Ekberg, and Brown by including the motivation of Blom because it would allow a subscriber and its associated home system authentication protocol, and a roamed system uses a corresponding local authentication protocol *[Blom, par. [001], lines 3-7]*.

Claim 15

Malinen further teaches the method of claim 14, wherein the step of obtaining from an electronic device a plurality of challenge response pairs comprises generating from a subscribed identify module (SIM) card a plurality of challenge response pairs and providing the SIM card to a user of the electronic device *[par. [0088], lines 2-3; a set of n SIM challenges, responses, and session keys may be used to create a key]*.

Claim 16

Blom further teaches the method of claim 14, wherein the step of providing response to a request for an authentication service a challenge response pair comprises vending the challenge response pair *[par. [0024], lines 21-25; a service provider is equivalent to a vendor]*.

Claim 17

Malinen further teaches the method of claim 14, wherein the step of providing response to a request for an authentication service a challenge response pair comprises securely communicating the challenge response pair to the service provider *[par. [0073]; par.*

[0074]; a client can use its own generated instance of the session key for secure communication with access provider. It is included to obtain a challenge response pair].

Action is Final

ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Conclusion

The prior arts made of record and not relied upon are considered pertinent to applicant's disclosure.

Please see attached PTO-892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Canh Le whose telephone number is 571-270-1380.

The examiner can normally be reached on Monday to Friday 7:30AM to 5:00PM other

Friday off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for

the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Canh Le
March 17, 2007